DETAILED ACTION

1. A response was received on 11 January 2011. By this response, Claim 1 has been amended. No claims have been added or canceled. Claims 1, 2, 4-8, 11, 14, and 16-18 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 11 January 2011 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 1, 2, 4-8, 11, 14, and 16-18 under 35 U.S.C. 103(a) as being unpatentable over Hattori, US Patent 6094632, in view of Higgins et al, “Speaker Verification Using Randomized Phrase Prompting”, and with specific reference to independent Claim 1, in response to applicant's arguments against the references individually (pages 9-12 of the present response), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

More specifically, Applicant separately argues that Hattori does not disclose generating one-time challenge phrases because, according to Applicant, Hattori does not disclose how the specified text is generated, and because the password is not random (pages 9-10 of the present response). However, even assuming *arguendo* that the above assertions are correct, Higgins was relied upon for disclosure of a database having a plurality of words and language rules for randomly generating one-time challenge phrases where each word of the phrase is randomly generated, as claimed.

Further with respect to Higgins, Applicant argues that the speech material in Higgins only includes 24 phrases from which the prompted phrases are selected, but that Higgins does not disclose generation of phrases wherein each word of the phrase is randomly generated (page 10 of the present response). However, the Examiner respectfully submits that this is an incorrect interpretation of the disclosures of Higgins. In particular, although Higgins does disclose that enrollment of a user requires speaking 24 phrases of three two-digit numbers each (page 90, section 2), Higgins does not disclose that the phrases generated for subsequent verification sessions must be selected from the 24 phrases that the user enrolled with. Rather, Higgins discloses that the prompted phrases are generated at random from the entire possible set of 56^3=175,616 phrases. In particular, Higgins states that there are 56^3 phrases and that "A verification trial or session consists of four such phrases" (page 90, section 2). This clearly does not limit the prompted phrases for the verification sessions to be selected from a subset of the phrases; rather, any of the 175,616 can be generated at random for verification trials. This is further supported by the description in Higgins of how verification is performed. The recognition vocabulary of the system is defined by partial words (see page 92, section 3.3.1, second paragraph), and the template matching is performed starting with a syntax that allows all 175,616 possible phrases (page 91, section 3.2, second paragraph). Further, templates for words are constructed by extracting tokens of the word spoken during enrollment and combining the tokens using an averaging procedure (see pages 95-97, section 3.4). All of these techniques would be unnecessary if the verification trials were limited to only the 24 phrases used in enrollment; however, the use of partial words and open syntax template matching allowing possible matching of all the 56^3 possible phrases clearly shows that any phrase from the vocabulary can be generated at random for a given verification trial. Higgins discloses nothing to suggest that only the 24 phrases used in enrollment can be used in subsequent verification trials.

Applicant further alleges that any modification of the text generation section of Hattori to generate a prompted phrase as in Higgins would not result in the database having a plurality of words and language rules for randomly generating one-time challenge phrases where each word in the phrase is randomly generated (page 10 of the present response). The Examiner respectfully disagrees, noting that, as detailed above, at least Higgins discloses a database having a plurality of words and language rules for randomly generating one-time challenge phrases as claimed (see Higgins, page 90, section 2, as previously cited, where phrases are generated at random subject to syntactic constraints).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., “Hattori does not disclose how the text generation section 201 is initiated”, see pages 10-11 of the present response) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claims do not explicitly recite any particular functionality of how a "text generation section… is initiated" or "what causes the text generation section… to start". With respect to the limitation of a station for receiving information representative of a user and generating a signal responsive thereto, Hattori discloses such a station (see Hattori, abstract, "A presentation section instructs the unknown speaker to input an ID").

Applicant further argues that Hattori individually discloses that two parts of the input pattern (i.e. the specified text and password) are processed separately and respectively for text verification and speaker recognition (pages 11-12 of the present response, citing Hattori, column 15, lines 10-50). However, the rejection acknowledged that Hattori does not explicitly disclose processing the entire signal for both speech and speaker recognition, and Higgins was instead relied upon to show this feature (see Higgins, pages 92-95, section 3.3 "Verification", especially the first paragraph, where it is determined whether the claimant was speaking, i.e. speaker recognition is performed, and whether the input utterance was spoken as prompted, i.e. speech recognition is performed to determine whether the exact challenge phrase was spoken).

Applicant further notes that the password in Hattori is not generated from a database and is not randomly generated (page 12 of the present response). However, it is noted that Applicant also clearly contemplated using a portion of a challenge phrase that was previously determined by a speaker and not randomly generated by the system; for example, Claims 6 and 7 of the present application explicitly recite that a user selects an additional phrase as a private, personal challenge phrase.

Regarding independent Claims 2, 4, 5, 16, and 17, and the claims depending therefrom, Applicant generally refers back to and/or repeats the arguments presented with respect to independent Claim 1 (see pages 12-14 of the present response), which have been addressed above.

Regarding dependent Claim 18, Applicant argues that Hattori does not disclose a plurality of words and language rules in a plurality of language sets as claimed, based on the allegation that Hattori only discloses a specific text of “December the twenty-fifth” (see page 14 of the present response, citing Hattori, column 9, lines 63-64). However, the Examiner submits that additional portions of Hattori do disclose the plurality of words and rules in a plurality of language sets as claimed (see, for example, Hattori, column 9, lines 19-47; column 8, line 65-column 9, line 5; column 9, lines 61-64, words and phrases in English; see also column 11, lines 18-37, disclosing use of Japanese language; the two languages are clearly different language sets having different words and rules).

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Claim Objections

3. Upon further consideration of the claims, the following objections are set forth.

4. Claims 1, 4, and 16-18 are objected to because of the following informalities:

Each of Claims 1, 4, and 16-18 uses the term “N-dimensional”; however, the variable “N” is not defined within the claims.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The rejection of Claim 1 under 35 U.S.C. 112, second paragraph, as indefinite is withdrawn in light of the amendments to the claim.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 2, 4-8, 11, 14, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hattori, US Patent 6094632, in view of Higgins et al, “Speaker Verification Using Randomized Phrase Prompting”.

In reference to Claim 1, Hattori discloses a biometric security system including a station for receiving input information, which is representative of a user, from the user and generating a signal responsive thereto (column 9, lines 5-11, where an ID is input);

a database having a plurality of words and language rules for randomly generating one-time challenge phrases (see column 9, lines 19-47; column 8, line 65-column 9, line 5, where "specified text" is provided to the user, which is a random phrase, see also column 9, lines 61-64); a database having biometric models of users (column 9, lines 5-20; column 11, lines 3-11, where a reference pattern of a registered speaker is stored; see also column 11, lines 17-42, and column 12, lines 14-54, noting the general references to plural speakers); and a controller that receives and validates the signal as representative of the user, where the controller communicates with the database that generates one-time challenge phrases for the user to speak exactly (column 8, line 65-column 9, line 5; column 9, lines 61-64), and communicates with the station to receive a spoken response and generate a second signal that represents the response (column 9, lines 5-11, the phrase is uttered by the unknown speaker), to validate voice information by speaker recognition (column 9, lines 21-28; column 11, lines 3-11) and verify voice information by speech recognition if the challenge phrase is matched exactly (column 9, lines 21-28; column 10, line 56-column 11, line 2), and to validate the spoken response to the challenge as representative of the user if the validation by speaker recognition and verification by speech recognition succeed (column 11, lines 12-16). However, Hattori does not explicitly disclose that each word in the one-time challenge phrase is randomly generated or processing the entire signal for both speech and speaker recognition.

Higgins discloses a biometric security system that includes a database having a plurality of words and language rules for randomly generating one-time challenge phrases (see page 90, section 2, where phrases are generated at random subject to syntactic constraints) and a controller that processes the entire signal received from the user for speaker recognition and speech recognition and validates the spoken response if both the validation by speaker recognition and verification by speech recognition succeed (see pages 92-95, section 3.3 “Verification”, where it is determined whether the claimant was speaking, i.e. speaker recognition is performed, and whether the input utterance was spoken as prompted, i.e. speech recognition is performed to determine whether the exact challenge phrase was spoken). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Hattori to include the random phrase generation and processing of the entire signal for speaker and speech recognition, as taught by Higgins, in order to have a robust algorithm (Higgins, page 89, section 1) and to prevent an imposter from knowing the prompted phrases in advance (Higgins, page 90, section 2).

Claims 2 and 7 are directed to methods corresponding substantially to the system of Claim 1, and are rejected by a similar rationale, noting further that Hattori and Higgins also disclose a private and personal challenge phrase (see Hattori, column 8, line 65-column 9, line 5).

In reference to Claim 8, Hattori and Higgins disclose everything as described above in reference to Claim 2. Neither Hattori nor Higgins explicitly discloses establishing a session time out limit; however, Official notice is taken, and it has been admitted as prior art due to the inadequate traversal of such Official notice, that it is well known in the art to establish a session time out in order to require that authentications must take place within a specific time period, so that the probability of an imposter being able to take more sophisticated deceptive actions is decrease. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Hattori to include a time out, in order to increase security and to realize the above noted predictable result.

In reference to Claim 4, Hattori discloses a biometric security system including a station for receiving input information, which is representative of a user, from the user and generating a first signal responsive thereto (column 9, lines 5-11, where an ID is input); a database having a plurality of words and language rules for randomly generating one-time challenge phrases (see column 9, lines 19-47; column 8, line 65-column 9, line 5, where “specified text” is provided to the user, which is a random phrase, see also column 9, lines 61-64); a database storing a biometric model of a user (column 9, lines 5-20; column 11, lines 3-11, where a reference pattern of a registered speaker is stored); and a controller receiving and validating the first signal, where the controller further randomly generates and forwards a word phrase as a challenge for a user to speak exactly (column 8, line 65-column 9, line 5; column 9, lines 61-64), receives and compares with the challenge a spoken response to the challenge (column 9, lines 5-11), and verifies the response as exactly matching the challenge (column 9, lines 21-28; column 10, line 56-column 11, line 2), and where the controller additionally validates the response if the response matches the stored model (column 9, lines 21-

28; column 11, lines 3-11), and the controller issues an authentication signal if both the response matches the phrase and the response is representative of the user (column 11, lines 12-16). However, Hattori does not explicitly disclose that each word in the one-time challenge phrase is randomly generated or processing the entire signal for both speech and speaker recognition.

Higgins discloses a biometric security system that includes a database having a plurality of words and language rules for randomly generating one-time challenge phrases (see page 90, section 2, where phrases are generated at random subject to syntactic constraints) and a controller that processes the entire signal received from the user for speaker recognition and speech recognition and validates the spoken response if both the validation by speaker recognition and verification by speech recognition succeed (see pages 92-95, section 3.3 “Verification”, where it is determined whether the claimant was speaking, i.e. speaker recognition is performed, and whether the input utterance was spoken as prompted, i.e. speech recognition is performed to determine whether the exact challenge phrase was spoken). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Hattori to include the random phrase generation and processing of the entire signal for speaker and speech recognition, as taught by Higgins, in order to have a robust algorithm (Higgins, page 89, section 1) and to prevent an imposter from knowing the prompted phrases in advance (Higgins, page 90, section 2).

In reference to Claim 18, Hattori further discloses storing words and language rules in a plurality of language sets specific to different subject areas (see, for example, column 9, lines 19-47; column 8, line 65-column 9, line 5; column 9, lines 61-64, words and phrases in English; see also column 11, lines 18-37, disclosing use of Japanese language).

Claims 5 and 6 are directed to methods corresponding substantially to the system of Claim 4, and are rejected by a similar rationale, noting that Hattori and Higgins disclose a multiplicity of users and stored biometric models (Hattori, column 11, lines 17-42, and column 12, lines 14-54, noting the general references to plural speakers), and noting further that Hattori and Higgins also disclose a private and personal challenge phrase (see Hattori, column 8, line 65-column 9, line 5, for example).

In reference to Claim 11, Hattori and Higgins disclose everything as described above in reference to Claim 5. Neither Hattori nor Higgins explicitly discloses establishing a session time out limit; however, Official notice is taken, and it has been admitted as prior art due to the inadequate traversal of such Official notice, that it is well known in the art to establish a session time out in order to require that authentications must take place within a specific time period, so that the probability of an imposter being able to take more sophisticated deceptive actions is decrease. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Hattori to include a time out, in order to increase security and to realize the above noted predictable result.

In reference to Claim 14, Hattori and Higgins disclose everything as described above in reference to Claim 5; however, neither Hattori nor Higgins explicitly discloses encrypting or digitally signing the spoken response. Official notice is taken, and it has been admitted as prior art due to the lack of traversal of such Official notice, that it is well known in the art to encrypt data when privacy of that data is needed and/or if that data will be sent over an insecure channel. Further, Official notice is taken, and it has been admitted as prior art due to the lack of traversal of such Official notice, that it is well known in the art to use a digital signature when it is necessary to verify the integrity of data, i.e. to make sure that the data has not been altered. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Hattori to include encryption, in order to increase the privacy and security of the data, and to include a digital signature, in order to allow the integrity of the data to be verified.

In reference to Claims 16 and 17, Hattori discloses a speech biometric security system including a station for receiving input information, which is representative of a user, from the user and generating a signal responsive thereto (column 9, lines 5-11, where an ID is input); a database having a plurality of words and language rules for randomly generating one-time challenge phrases (see column 9, lines 19-47; column 8, line 65-column 9, line 5, where “specified text” is provided to the user, which is a random phrase, see also column 9, lines 61-64); a database having biometric models of users (column 9, lines 5-20; column 11, lines 3-11, where a reference pattern of a registered speaker is stored; see also column 11, lines 17-42, and column 12, lines 14-54, noting the general references to plural speakers); and a controller that receives and validates the signal as representative of the user, where the controller communicates with the database that generates one-time challenge phrases for the user to speak exactly (column 8, line 65-column 9, line 5; column 9, lines 61-64), and communicates with the station to receive a spoken response and generate a second signal that represents the response (column 9, lines 5-11), to process the response by speaker recognition and issue a first validation signal in response to a match between the spoken response and a stored biometric model (column 9, lines 21-28; column 11, lines 3-11) and simultaneously process the response by speech recognition and issue a second validation signal if the spoken response exactly matches the challenge phrase (column 9, lines 21-28; column 10, line 56-column 11, line 2), and issue a positive authentication signal in response to the first and second validation signals (column 11, lines 12-16). However, Hattori does not explicitly disclose that each word in the one-time challenge phrase is randomly generated or processing the entire signal for both speech and speaker recognition.

Higgins discloses a biometric security system that includes a database having a plurality of words and language rules for randomly generating one-time challenge phrases (see page 90, section 2, where phrases are generated at random subject to syntactic constraints) and a controller that processes the entire signal received from the user for speaker recognition and speech recognition and validates the spoken response if both the validation by speaker recognition and verification by speech recognition succeed (see pages 92-95, section 3.3 “Verification”, where it is determined whether the claimant was speaking, i.e. speaker recognition is performed, and whether the input utterance was spoken as prompted, i.e. speech recognition is performed to determine whether the exact challenge phrase was spoken). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Hattori to include the random phrase generation and processing of the entire signal for speaker and speech recognition, as taught by Higgins, in order to have a robust algorithm (Higgins, page 89, section 1) and to prevent an imposter from knowing the prompted phrases in advance (Higgins, page 90, section 2).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Hoffman, US Patent 7882032, discloses a system for authentication that includes prompting a user to speak several randomly selected words.

b. Matsui et al, “Concatenated Phoneme Models for Text-Variable Speaker Recognition”, discloses techniques for speaker recognition that include key text that is changed with each use.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Primary Examiner, Art Unit 2492